REMARKS

Claims 1-31 were pending in the patent application. By this amendment, Applicants have canceled Claims 1-8 and 27-29, and 31. The Examiner has rejected Claim 9, and Claims 10 and 11 which depend therefrom, under 35 USC 112, concluding that the term "directly" is not supported by the Specification. While the meaning of the claim language will be discussed in greater detail below, for purposes of the 112 rejection, Claim 9 has been amended.

The Examiner has additionally rejected Claim 29 under 35 USC 112 since no antecedent basis exists for the term "generating". Applicants have canceled Claim 29.

The Examiner has rejected Claims 1, 3, 4, 6, 7, 9-11, and 31 under 35 USC 102(b) as anticipated by the Merritt patent; Claim 27 (now canceled) under 35 USC 102(b) as being anticipated by the Pfitzmann reference; Claim 2 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Pfitzmann; Claims 5 and 8 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Giltner; Claims 12-19, 21-22, and 26 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Manduley; Claims 23 and 24 as being unpatentable over

Merritt in view of Manduley and Schneier; Claim 20 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Manduley further in view of Lessin; Claim 25 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Manduley and further in view of Daggar; Claims 28 and 30 (now canceled) as being unpatentable over Pfitzmann in view of Konigs and Manduley; and Claim 29 (now canceled) as unpatentable over Pfitzmann in view of Konigs. For the reasons set forth below, Applicants respectfully assert that the claims, as amended, are patentable over the cited art. With regard to the amendments to Claim 30, Applicants have amended the program storage device language of the claim to parallel the language of method Claim 12. Accordingly, the rejection of Claim 30 as unpatentable over Pfitzmann in view of Konigs and Manduley does not apply. The language of Claim 30 will be defended as if the Examiner rejected Claim 30 using the same art used to reject Claim 12.

The present invention teaches and claims a device, terminal, server, program storage device, and method for establishing trustworthy connections among a user, with or without a device inserted at a terminal, a terminal, and a server. Specifically, the user must know that the terminal

is trusted by the server before the user will release any sensitive information to the terminal. Similarly, the server must know that the terminal seeking access to it is authentic. The server may also engage in an exchange to determine if the user, of a user device or of the terminal, is authorized to access the server. In all claimed embodiments of the invention, the server authenticates the terminal. Once the terminal has been authenticated, the server either communicates that information directly to the user by display at the user device, or communicates that information to the user by notifying the user device whereupon the user device causes the terminal to display the information to the user, when the user has a device that does not have display capabilities. Applicants respectfully assert that none of the cited prior art teaches or suggests a server communicating terminal authentication information directly to the user device. Applicants also assert that none of the prior art teaches or suggests that terminal authentication information be communicated to the user, whereupon the user or user device provides information to the terminal for the terminal to dynamically create a user-specific authenticity output message for display to the

user. None of the cited art teaches or suggests that a terminal dynamically create an authenticity output message.

The primary reference cited against the present application is the Merritt patent. The Merritt patent teaches a method for authenticating a terminal whereby a terminal contacts the server, the server provides a user-specific personal security phrase ("PSP") to the terminal and the terminal displays the PSP to the user. Under the Merritt method, the server does not communicate authentication information directly to a user device. Further, under the Merritt method, the terminal does not dynamically create an authenticity output message. Rather, the Merritt terminal outputs a server-generated message.

Applicants respectfully assert that the Merritt patent does not teach or suggest the invention as claimed. The claimed invention expressly recites that the server provides terminal authentication information directly to the user device (Claims 9-26, and 30). Claim 18 further expressly recites that the user device provides user-specific information to the terminal, after receiving terminal authentication information from the server, for use by the terminal in dynamically creating the authenticity output message.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Merritt patent does not teach that the server provides terminal authentication information directly to the user device, does not teach that a user device provides user-specific information to the terminal for the terminal to dynamically create the authenticity output message, and does not teach that a user device authenticate a user, it cannot be maintained that the Merritt patent anticipates the invention as claimed.

Applicants further assert that the additionally cited patents do not provide the teachings which are missing from the Merritt patent. With respect to the Manduley patent, Applicants contend that the combination of Merritt and Manduley does not obviate the invention as claimed. The Examiner acknowledges that the Merritt patent does not teach or suggest providing a terminal authenticity message to the device. The Manduley patent has been cited for teaching a method for assuring that the user is actually in possession of the card. However, that is NOT what is being claimed. The invention as set forth in independent claim 12 expressly recites the server providing a terminal authenticity message

to the device via the established second trusted connection. As claimed, the user device is being provided with confirmation that the terminal has been authenticated. User authentication is not being claimed. Moreover, sending terminal authentication information directly from a server to a user device, thereby eliminating the possibility of a terminal interfering with or falsely generating a terminal authentication message, is not taught or suggested by the Manduley authentication. The Examiner has concluded that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to send the authenticity output message to the smart card...and because the legitimate user of the card will be reading the messages". However, neither Manduley nor Merritt teaches that a terminal authentication message be communicated directly to the user along a connection between the user and the server, without also communicating the message along the connection between the terminal and the server. Since that limitation is not taught or suggested by the cited references, and since that limitation is recited in all of the remaining pending claims, it cannot be concluded that the claims are rendered obvious by the combination of teachings of Merritt and Manduley.

Even if one were to combine the teachings of Merritt and Manduley, one would not arrive at the invention as claimed. The combination would produce a Merritt system wherein a user is first authenticated to the terminal, and then the terminal would proceed to seek its own authentication from the server for presentation, in the form of the PSP, to the user. Such would effectively teach away from the present invention since, by having the Manduley user authentication up front, the user would be forced to provide secure information to an untrusted terminal. Further, since the terminal would seek its authentication from the server, and would then presumably communicate that authentication to the user, there is no way for the user to independently (i.e., with direct communication from the server to the user/device without communication to the terminal) verify that the terminal has been authenticated.

The addition of the teachings of the Schneier reference to the combination of Merritt and Manduley do not render the invention obvious. While Schneier can output a number to represent a message, there is nothing in Schneier which would lead one having skill in the art to modify the combination of Merritt and Manduley to include communication of terminal authentication along a connection between a

server and a user device and not along a different connection between the terminal and the server.

The addition of the Lessin patent teachings to the combination of Merritt and Manduley does not render the pending claims obvious. Lessin has been cited for teaching that a user enter a PIN. The combination of Merritt, Manduley and Lessin would again effectively teach away from the claimed invention since the user would be forced to enter his PIN at a terminal before establishing that the terminal was trusted. Clearly that does not obviate the language of Claim 20, which expressly states that the server first send terminal authentication information directly to the user, apart from the user device-and not the terminal-authenticating the user.

Similarly, the addition of Daggar to the combination of Merritt and Manduley would not obviate the invention as set forth in Claim 25. Daggar simply states that card authenticity must be established. Daggar neither teaches nor suggests how Daggar would establish the authenticity of the card. Moreover, it cannot be concluded that the claimed implementation is obviated since the claim recites the limitations of Claim 12 further comprising authenticating the device to the server. Since none of the cited

references teaches that the device be authenticated, that the server establish a trusted connection with the device and that the server communication terminal authentication information directly to the device along the trusted connection, it cannot be concluded that the combination obviate the claim.

In the ***Response to Arguments*** section, the Examiner has stated that the feature upon which Applicants rely, namely that the device has its own authentication component, is not recited in Claim 25. Applicants respectfully disagree. While Claim 25 does not expressly state that a device has an authentication component, Claim 12 from which Claim 25 depends recites "at least one server which is authenticatable by said device."

With regard to the arguments that the terminal authentication is sent directly from a server to the device/user, both in the ***Response to Arguments*** section and with regard to the 112 rejection of Claim 9, Applicants note that the term "directly" was chosen to refer to direct communication between the authenticating server and the user along the second connection, without involvement of or notice to the terminal along the first connection. Support for this argument is found in the original Specification at

page 10, line 22-page 23, line 2, and page 12, lines 14-15. In the claimed embodiment, which is taught therein, the authenticity output message is sent along the second connection, which is the direct connection between the serve r and the device (Claims 9-26 and 28), without the terminal being involved. In one embodiment, the authenticity output message is displayed by the device to the user (Claims 9-11, 14, 21, 23 and 28), again without the terminal being involved, which may be desirable for security purposes so that the terminal is prevented from interfering with or falsely generating a terminal authentication message. Alternative embodiments teach and claim that the authenticity output message be conveyed to the terminal, for example when the user device does not have output capabilities or when the user does not have a device (see: page 13, line 21-page 22).

Applicants note that, even if the second connection is tunneled through the first connection, the two connections are distinct "lines" of communication, and communications send along the first connection are not also necessarily sent along the second connection, and vice versa. While the two connections may share physical links, they do not share communications. When the server sends a message to the user

device along the second connection, that message does not go along the first connection and is not received at the terminal. Even if the second connection is tunneled through the first connection, the server can communicate with the terminal along the first connection without the message going along the second connection to the user device. If a message from the server was intended for both the user device and the terminal, two messages would be sent, one along each connection. Accordingly, sending a message "directly" to a destination along either the first or the second connection means sending it ***only*** to the destination which is linked to the server by that connection.

The Examiner also concludes, in the ***Response to Arguments*** section, that "[w]hile the information from the user's card is given to the terminal before authentication, the claims do not state that the terminal must be trusted *before* the user accesses the terminal". Applicants respectfully assert that a user can access a terminal and through the terminal access the server to obtain terminal authentication before terminal authentication. The user may access the terminal but will not input certain sensitive information to the terminal until the user has received the terminal authentication output message. Applicants are not

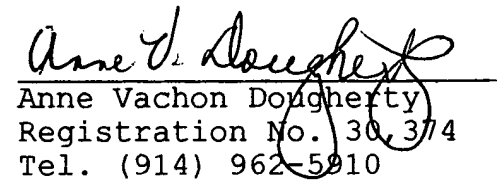
claiming that a terminal must be trusted before it is accessed, since such may simply not be possible when a user does not have a stand-alone device. Rather, Applicants are claiming a system and method for establishing a trustworthy connection between a user having a personal device and a terminal.

Finally, the Examiner states, in the ***Response to Arguments*** section, that "the claims do not recite a limitation where a user is only inclined to enter personal information, such as a pin to the terminal after the authentication message has arrived." Since Applicants are claiming the server and method performed by the server, entry of user's personal information to a terminal is not part of the server functionality. Moreover, entry of user's personal information to a terminal would only occur *after* execution of the inventive method. Applicants believe that the patentability of the invention does not hinge on the post-authentication entry of user personal information and consequently have not included claim language to that effect.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

N. Asokan, et al

By: 

Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910